Small Business Innovation Research/Small Business Tech Transfer

Formal Verification of Interactions of the RTOS, Memory System, and Application Programs at the PowerPC 750 Binary Code Level, Phase I

Completed Technology Project (2013 - 2013)

Project Introduction

In the proposed project, we will formally verify the correctness of the interaction between a Real-Time Operating System (RTOS) and user processes under various operating scenarios, such as multitasking, interrupt handling, user and kernel mode switching. The formal verification will be done assuming execution on the PowerPC 750 architecture that is implemented in the radiation-hardened RAD750 flight-control computers utilized in many NASA space missions, and are planned to be used in future spacecraft, including the Orion Multi-Purpose Crew Vehicle. A unique advantage of our project will be that the formal verification will precisely account for the bit-level semantics of all instructions, as well as the memory system, the bus, and devices on the bus, including multiple CPUs, and thus will allow us to precisely analyze all possible behaviors of the entire system, which is critical for aerospace applications. During Phase I we will lay the foundation for Phase II by: developing initial models of the memory system and the bus; formally defining the bit-level semantics of additional instructions from the PowerPC 750 architecture that we have not specified yet; identifying properties that we will prove to guarantee correct interaction of user processes with the target RTOS, the memory system, and the bus, including scenarios such as multitasking, interrupt handling, user and kernel mode switching; proving some of these properties; and identifying the most promising directions for Phase II work.

Primary U.S. Work Locations and Key Partners

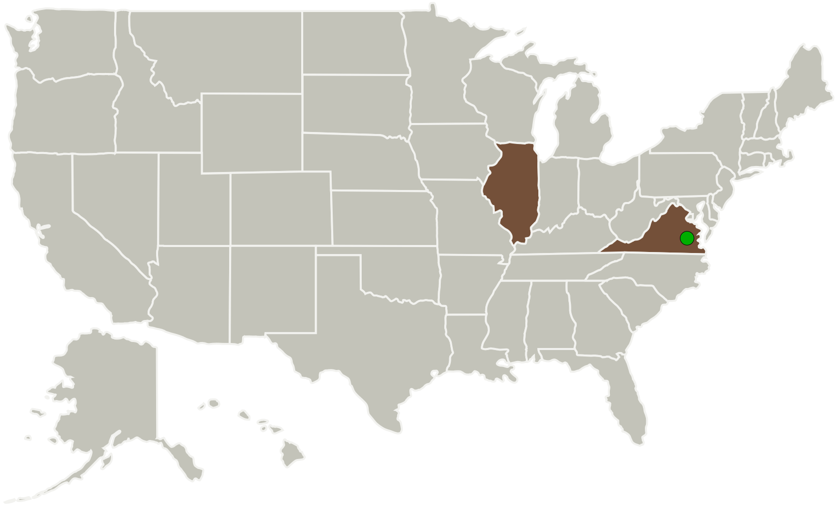


Table of Contents

Organizational Responsibility

Responsible Mission Directorate:

Space Technology Mission Directorate (STMD)

Lead Organization:

Aries Design Automation, LLC

Responsible Program:

Small Business Innovation Research/Small Business Tech Transfer

Project Management

Program Director:

Jason L Kessler

Program Manager:

Carlos Torrez

Continued on following page.

Organizations Performing Work	Role	Type	Location
Aries Design Automation, LLC	Lead Organization	Industry	Chicago, Illinois
●Langley Research Center(LaRC)	Supporting Organization	NASA Center	Hampton, Virginia

Primary U.S. Work Locations	
Illinois	Virginia

Project Transitions

May 2013: Project Start

November 2013: Closed out

Closeout Documentation:

- Final Summary Chart*(https://techport.nasa.gov/file/138173)*

Images

Project Image

Formal Verification of Interactions of the RTOS, Memory System, and Application Programs at the PowerPC 750 Binary Code Level *(https://techport.nasa.gov/image/129935)*

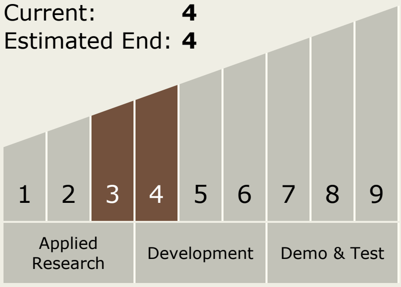
Project Management *(cont.)*

Principal Investigator:

Miroslav N Velev

Technology Maturity (TRL)

Start: **3**
Current: **4**
Estimated End: **4**



Technology Areas

Primary:

- TX11 Software, Modeling, Simulation, and Information Processing
  └ TX11.2 Modeling
    └ TX11.2.1 Software Modeling and Model Checking

Target Destinations

The Sun, Earth, The Moon, Mars, Others Inside the Solar System, Outside the Solar System